AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) In a computer system that ~~including~~ includes a plurality of initiators, each for initiating communication with target devices over a network, a method for configuring the computer system to securely communicate with a target device over the network, the method comprising the following performed by an abstraction module that configures each of the plurality of initiators in a manner that security conflicts between the plurality of initiators is avoided:

an act of exposing a common interface that may be used to configure any of the plurality of initiators;

an act of receiving an indication through the common interface that a selected initiator from among the plurality of initiators is to be configured to communicate with a selected target device;

an act of retrieving security information from a database that includes information that is relevant to configuring security for any of the plurality of initiators;

an act of identifying a security configuration of the selected initiator using the retrieved security information;

an act of determining that if the identified security configuration were applied to the selected initiator, the applied identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators; and

upon determining that the identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators, an act of configuring the selected initiator using the identified security configuration.

2. (Original) A method in accordance with Claim 1, wherein the identified security configuration is different than the retrieved security information.

3. (Original) A method in accordance with Claim 1, wherein the identified security configuration is the same as the retrieved security information.

4. (Original) A method in accordance with Claim 1, wherein the retrieved security information comprises IPSec configuration information.

5. (Currently Amended) A method in accordance with Claim 1, wherein the retrieved security information comprising CHAP configuration information.

6. (Original) A method in accordance with Claim 1, wherein the selected initiator is configured to cause communication to occur with the target device using iSCSI.

7. (Original) A method in accordance with Claim 1, wherein the act of retrieving security information from a database comprises an act of retrieving the security information from an Active Directory.

8. (Original) A method in accordance with Claim 1, wherein the selected initiator is a hardware initiator.

9. (Original) A method in accordance with Claim 1, wherein the selected initiator is a software initiator.

10. (Original) A method in accordance with Claim 1, wherein the act of retrieving security information occurs in response to the act of the abstraction module receiving the indication.

11. (Original) A method in accordance with Claim 1, wherein the indication through the common interface is received in response to a request to communicate with the selected target device.

12. (Original) A method in accordance with Claim 1, wherein the indication through the common interface is received in advance of any express request to communicate with the selected target device.

13. (Original) A method in accordance with Claim 12, wherein the indication through the common interface is received in response to initializing the computer system.

14. (Currently Amended) In a computer system that ~~including~~ includes a plurality of initiators, each for initiating communication with target devices over a network, a method for configuring the computer system to securely communicate with a target device over the network, the method comprising the following performed by an abstraction module that configures each of the plurality of initiators in a manner that security conflicts between the plurality of initiators is avoided:

an act of exposing a common interface that may be used to configure any of the plurality of initiators;

an act of receiving an indication through the common interface that a selected initiator from among the plurality of initiators is to be configured to communicate with a selected target device; and

a step for causing the selected initiator to communicate with the selected target device using security settings that ~~such that the security configuration of the selected initiator~~ does not conflict with security configurations of others of the plurality of initiators such that the security configuration of the selected initiator is consistent with the security configurations of others of the plurality of initiators.

15. (Currently Amended) A method in accordance with Claim 14, wherein the step for causing the selected initiator to communicate with the selected target device comprises the following:

an act of retrieving security information from a database that includes information that is relevant to configuring security for any of the plurality of initiators;

an act of identifying a security configuration of the selected initiator using the retrieved security information;

an act of determining that if the identified security configuration were applied to the selected initiator, the applied identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators; and

upon determining that the identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators, an act of configuring the selected initiator using the identified security configuration.

16. (Original) A method in accordance with Claim 15, wherein the identified security configuration is different than the retrieved security information.

17. (Original) A method in accordance with Claim 15, wherein the identified security configuration is the same as the retrieved security information.

18. (Original) A method in accordance with Claim 15, wherein the retrieved security information comprises IPSec configuration information.

19. (Original) A method in accordance with Claim 15, wherein the retrieved security information comprising CHAP configuration information

20. (Original) A method in accordance with Claim 15, wherein the selected initiator is configured to cause communication to occur with the target device using iSCSI.

21. (Original) A method in accordance with Claim 15, wherein the act of retrieving security information from a database comprises an act of retrieving the security information from an Active Directory.

22. (Original) A method in accordance with Claim 15, wherein the selected initiator is a hardware initiator.

23. (Original) A method in accordance with Claim 15, wherein the selected initiator is a software initiator.

24. (Currently Amended) A computer program product for use in a computer system that ~~including~~ includes a plurality of initiators, each for initiating communication with target devices over a network, the computer program product for implementing a method for configuring the computer system to securely communicate with a target device over the network, the computer program product comprising one or more computer-readable media having thereon computer-executable instructions that, when executed by one or more processors of the computing system, cause the computing system to perform the following:

an act of instantiating an abstraction module and causes the abstraction module to perform the following:

an act of exposing a common interface that may be used to configure any of the plurality of initiators;

an act of receiving an indication through the common interface that a selected initiator from among the plurality of initiators is to be configured to communicate with a selected target device;

an act of retrieving security information from a database that includes information that is relevant to configuring security for any of the plurality of initiators;

an act of identifying a security configuration of the selected initiator using the retrieved security information;

an act of determining that if the identified security configuration were applied to the selected initiator, the applied identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators; and

upon determining that the identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators, an act of configuring the selected initiator using the identified security configuration.

25. (Original) A computer program product in accordance with Claim 24, wherein the one or more computer-readable media are physical memory media.

26. (Original) A computer program product in accordance with Claim 25, wherein the one or more computer-readable media is persistent memory.

27. (Original) A computer program product in accordance with Claim 25, wherein the one or more computer-readable media is volatile system memory.

28. (Original) A computer program product in accordance with Claim 24, wherein the retrieved security information comprises IPSec configuration information.

29. (Original) A computer program product in accordance with Claim 24, wherein the retrieved security information comprising CHAP configuration information.

30. (Currently Amended) A computer program product for use in a computer system that ~~including~~ includes a plurality of initiators, each for initiating communication with target devices over a network, the computer program product for implementing a method for configuring the computer system to securely communicate with a target device over the network, the computer program product comprising one or more computer-readable media having thereon computer-executable instructions that, when executed by one or more processors of the computing system, cause the computing system to instantiate the following:

a plurality of initiators, each capable of communicating with at least one of the plurality of target devices;

an abstraction module configured to expose a common interface that may be used to configure any of the plurality of initiators, receive an indication through the common interface that a selected initiator from among the plurality of initiators is to be configured to communicate with a selected target device, retrieve security information from a database that includes information that is relevant to configuring security for any of the plurality of initiators, identify a security configuration of the selected initiator using the retrieved security information in response to receiving the indication, determine that if the identified security configuration were applied to the selected initiator, that the applied identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators, and, upon determining that the identified security configuration would not cause the selected initiator to conflict with any of the existing security configurations of the other of the plurality of initiators, configure the selected indicator using the identified security configuration ~~if the identified security information would not cause the selected initiator to conflict with any of the other of the plurality of initiators~~.

31. (Original) A computer program product in accordance with Claim 30, wherein the one or more computer-readable media further have thereon computer-executable instructions that, when executed by one or more processors of the computing system, cause the computing system to instantiate the following:

a software module configured to submit the indication to the common interface.

32. (Original) A computer program product in accordance with Claim 30, wherein the one or more computer-readable media are physical memory media.

33. (Original) A computer program product in accordance with Claim 32, wherein the one or more computer-readable media is persistent memory.

34. (Original) A computer program product in accordance with Claim 32, wherein the one or more computer-readable media is volatile system memory.